

# Catalyst 3550 シリーズ スイッチ上の 802.1x 有線認証と ACS バージョン 4.2 の設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[スイッチの設定例](#)

[ACS 設定](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Cisco Access Control Server ( ACS ) バージョン 4.2 と有線認証用の Remote Access Dial In User Service ( RADIUS ) プロトコルを使用した基本的な IEEE 802.1x 設定例を示します。

## 前提条件

### 要件

シスコでは次を推奨しています。

- ACS とスイッチの間の IP 到達可能性を確認する。
- ACS とスイッチの間で User Datagram Protocol ( UDP ) ポート 1645 および 1646 が開いていることを確認する。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst 3550 シリーズ スイッチ
- Cisco Secure ACS バージョン 4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### スイッチの設定例

1. RADIUS サーバと事前共有キーを定義するために、次のコマンドを入力します。

```
Switch(config)# radius-server host 192.168.1.3 key cisco123
```

2. 802.1x 機能を有効にするために、次のコマンドを入力します。

```
Switch(config)# dot1x system-auth-control
```

3. 認証、認可、およびアカウントリング (AAA) と RADIUS の認証および認可をグローバルに有効にするために、次のコマンドを入力します。  
注：これはRADIUSサーバから属性を渡す必要がある場合に必要です。それ以外の場合はスキップできます。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

### ACS 設定

1. ACS にスイッチを AAA クライアントとして追加するために、[Network Configuration] > [Add entry AAA client] に移動し、次の情報を入力します。  
IPアドレス:<IP>共有秘密:<key>Radius(Cisco IOS<sup>®</sup>/PIX 6.0)を使用した認証

**Network Configuration**

AAA Client Hostname: switch  
 AAA Client IP Address: 192.168.1.2  
 Shared Secret: cisco123

**RADIUS Key Wrap**  
 Key Encryption Key: [ ]  
 Message Authenticator Code Key: [ ]  
 Key Input Format:  ASCII  Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Right sidebar text:  
 You can use the wildcard asterisk (\*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.\* in the AAA Client IP Address box.  
 You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.  
[\[Back to Top\]](#)  
**Shared Secret**  
 The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and ACS identically, including case sensitivity.  
[\[Back to Top\]](#)  
**Network Device Group**  
 From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.  
 Note: To enable NDGs, click **Interface Configuration > Advanced Options > Network Device Groups**.  
[\[Back to Top\]](#)  
**RADIUS Key Wrap**

2. 認証設定を指定するために、[System Configuration] > [Global Authentication Setup] に移動し、[Allow MS-CHAP Version 2 Authentication] チェックボックスがオンになっていることを確認します。

**System Configuration**

EAP-TLS session timeout (minutes): 120

Select one of the following options for setting username during authentication:  
 Use Outer Identity  
 Use CN as Identity  
 Use SAN as Identity

**LEAP**  
 Allow LEAP (For Aironet only)

**EAP-MD5**  
 Allow EAP-MD5

AP EAP request timeout (seconds): 20

**MS-CHAP Configuration**

- Allow MS-CHAP Version 1 Authentication
- Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

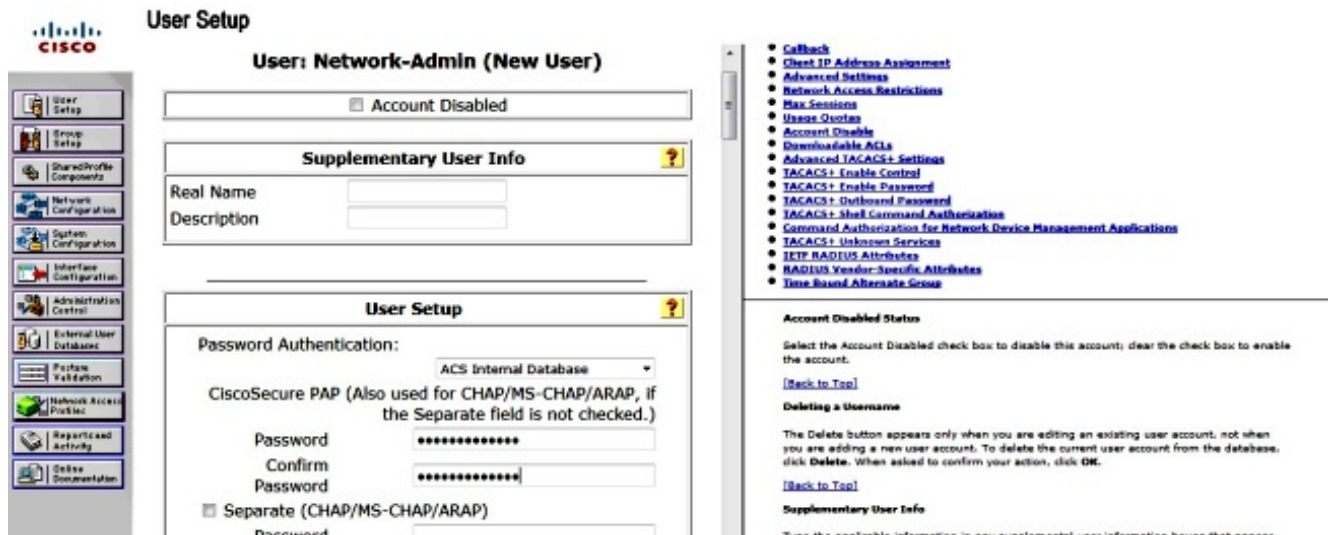
Right sidebar text:  
 Use this page to specify settings for various authentication protocols.  

- [EAP Configuration](#)
- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP-EAP Request Timeout](#)
- [MS-CHAP Configuration](#)

**EAP Configuration**  
 EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.  
[\[Back to Top\]](#)  
**PEAP**  
 PEAP is the outer layer protocol for the secure tunnel.  
 Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the [ACS Certificate Setup page](#).  

- **Allow EAP-MSCHAPv2** - Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** - Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow Dynamic Validation** - Use to enable the DPAD (PAP-TLV) protocol for dynamic validation of

3. ユーザを設定するために、メニューの [User Setup] をクリックし、次の手順を実行します。User情報としてNetwork-Admin <username>を入力します。[Add/Edit] をクリックします。[Real Name] にNetwork-Admin <description name>と入力します。Description: <your choice>を追加します。Password Authentication:ACS Internal Databaseを選択します。[Password] に「. . .」と入力します。..... <password>。Password: <password>を確認します。[Submit] をクリックします。



## 確認

アウトプット インタープリタ ツール ( 登録ユーザ専用 ) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

設定が正常に機能していることを確認するには、次のコマンドを入力します。

- **show dot1x**
- **show dot1x summary**
- **show dot1x interface**
- **show authentication sessions interface <interface>**
- **show authentication interface <interface>**

```
Switch(config)# show dot1x
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

```
Switch(config)# show dot1x summary
```

```
Interface PAE Client Status
```

```
Fa0/4 AUTH
```

```
Switch(config)# show dot1x interface fa0/4 detail
```

```
Dot1x Info for FastEthernet0/4
```

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

# トラブルシュート

ここでは、設定をトラブルシューティングするために使用できる debug コマンドを示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- debug dot1x all
- debug authentication all
- debug radius ( デバッグ レベルで RADIUS の情報を提供 )
- debug aaa authentication ( 認証のデバッグ )
- debug aaa authorization ( 認可のデバッグ )

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。